



# Complexity and Security in ICT Systems

(work in progress)



**Michael H. Behringer, Distinguished Engineer, Cisco Systems**

**2<sup>nd</sup> FORWARD Workshop**

**4<sup>th</sup> May 2009, Nice, France**

# Complexity on a Router

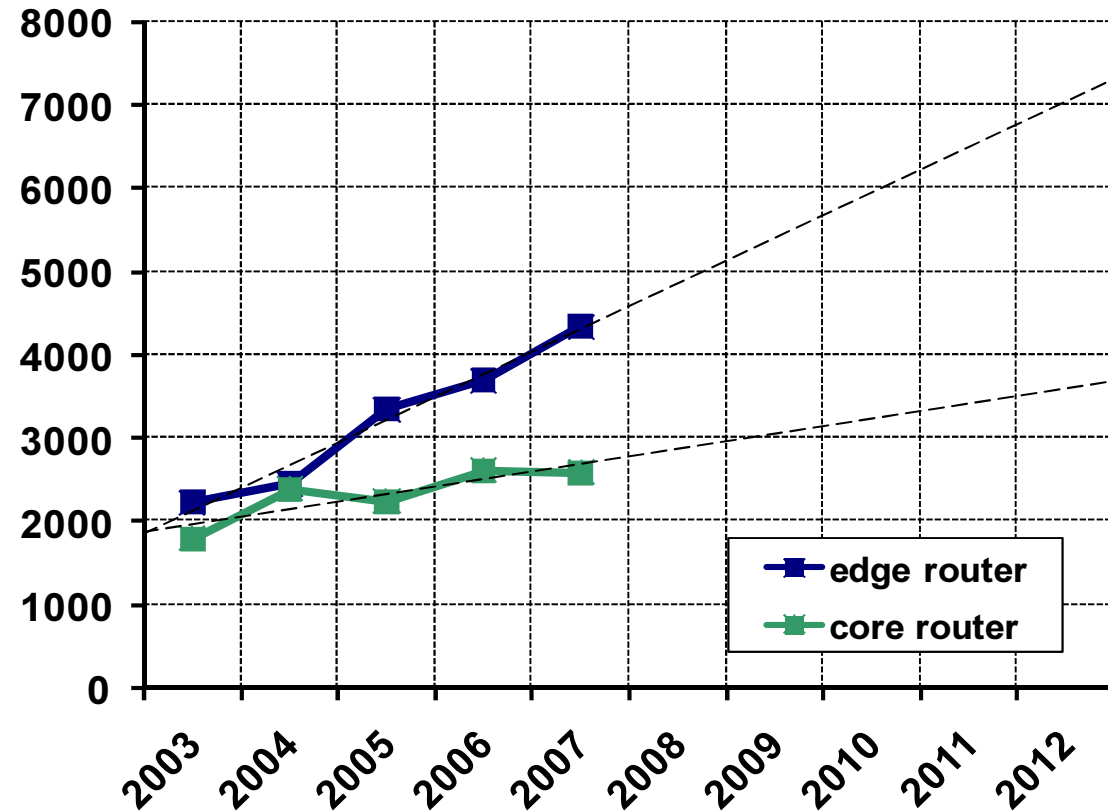
- Length of configuration
- Size of OS
- Number of features
- Number of data structures
  - FIB, LFIB, RIB (per protocol), ARP table
- Number of transmission techniques
  - ADSL, VDSL, POS, X.25, ATM, L2TP, PPPoX, ...
- ...

# Length of Router Configuration

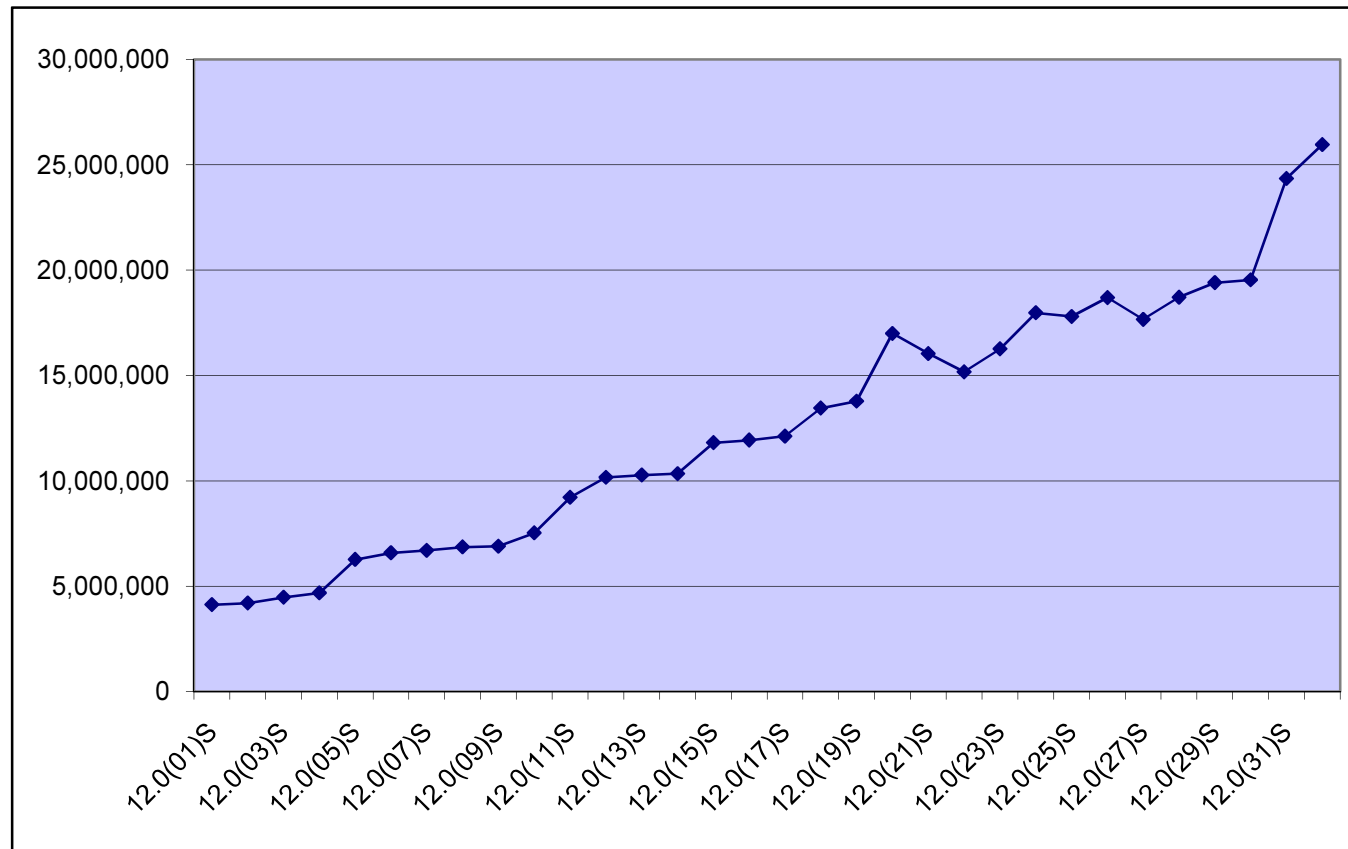
Example: Tier-2 SP (EU)

lines of configuration of:

- a typical metro ethernet edge router
  - doubles in ~ 4 years
- a typical core router
  - doubles in ~ 10 years

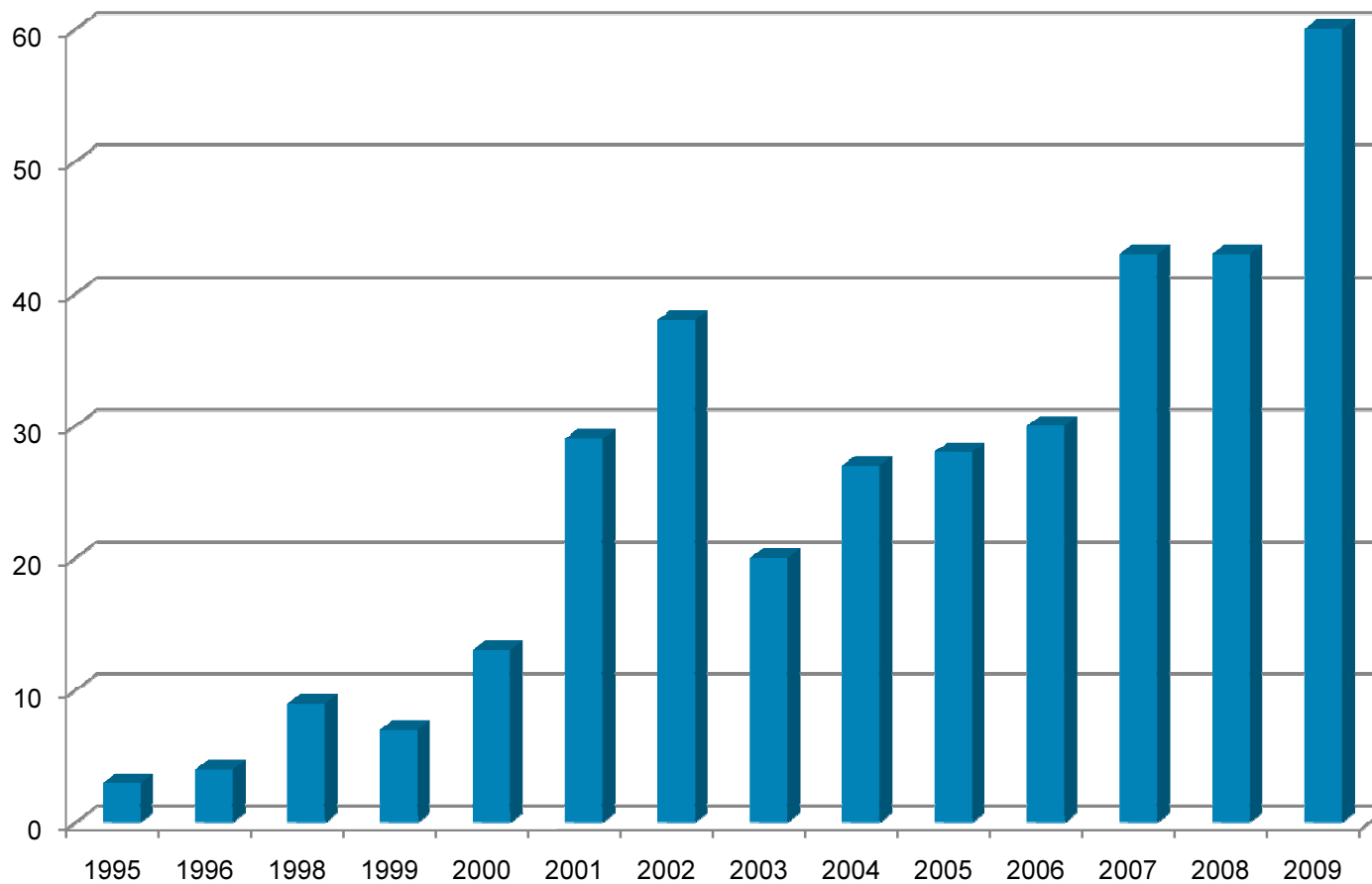


# Size of the Operating System



Example: Cisco IOS 12.0S release train  
(size of executable file in bytes)

# Number of Vulnerabilities



Note: This graph reflects a growing product range over time. There were also changes in the evaluation type over time. Use these data with care!

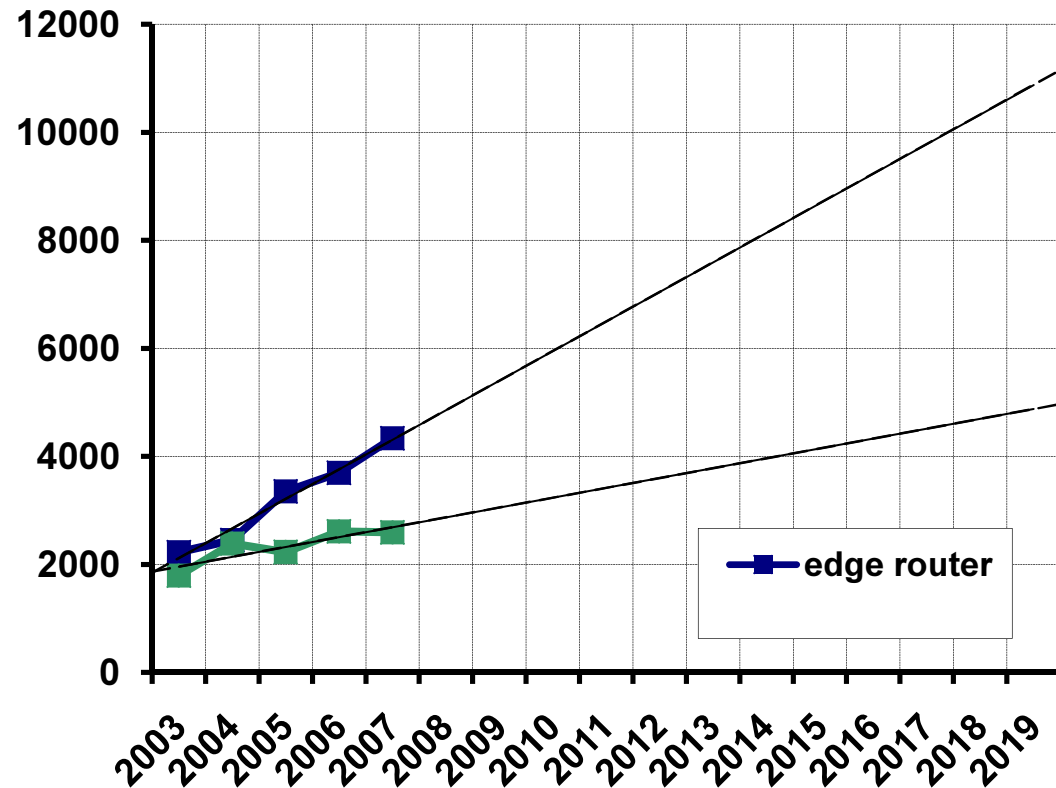
projected as of  
April 2009

# Complexity on the Internet / a Network

- Number of routed prefixes
- Number of routed autonomous systems (AS)
- Number of AS paths
- AS / prefix Churn
- Number of network elements on a path
- Number of protocols (IPv4, IPv6)
- ...

# Some Projections\*: In 10 years...

- core router config:  
~ 5,000 lines
- edge router config:  
~11,000 lines
- Cisco will issue:  
~80 advisories / year



\* all assumig linear growth

# Lessons Learned So Far\*

- Difficult to understand networks, traffic, logs, routing, switching, security measures, ...
- Humans are bad at iterative jobs  
Example: Security log evaluation
- Generally, automated systems more reliable than humans  
Example: Translating security policy into packet filters; log evaluation
- Generally, protocols more reliable than manual configuration  
Example: Troubleshooting IPsec

\* subjective view of the author

# Determinism and Reality\*

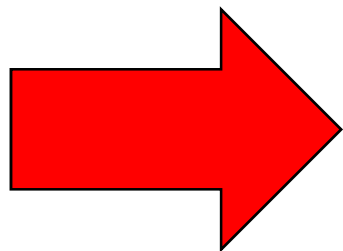
- 10 years ago, security decisions were deterministic  
“block file transfer / block FTP”
  - Today hard to be deterministic:  
Protocols are increasingly complex, encrypted, hard to parse  
(Try to block illegal file downloads!)  
Many false negatives
  - Consider: Service provider aggregation router  
In 10 years, impossible to scan and parse traffic for malware,  
bots, attacks, etc.
- Need new, non-deterministic forms of decisions:  
E.g., reputation

\* subjective view of the author

# Interim “Conclusion”

(Disclaimers: “work in progress”; “highly subjective”)

- Humans cannot manually:  
Configure, troubleshoot, secure.
- Need to research:  
Complete automation of network management  
Complete automation of security monitoring  
Complete automation of security incident handling  
New, non-deterministic ways of making decisions (eg, reputation)



**Mission critical ICT systems must be managed and secured automatically, with little or no human intervention**